

United States Patent Application

of

Leo J. Campbell

and

Jon L. Cook

for

Methods and Systems for Proofing Identities

Using a Certificate Authority

Attorney for Applicants

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

I. RELATED APPLICATIONS

This application claims the benefit of U.S. Provisional Patent Application No. 60/189,983 with a filing date of March 17, 2000, which is incorporated herein by reference.

II. BACKGROUND OF THE INVENTION

A. Field of the Invention

The present invention relates to systems and methods for providing electronic communications to a customer. More particularly, the invention relates to systems and methods for providing an electronic account and other services to a customer by linking the customer's electronic address to a physical address where the customer receives physical mail.

B. Description of the Related Art

The United States Postal Service (USPS) is an independent government agency that provides mail delivery and other services to the public. The USPS is widely recognized as a safe and reliable means for sending and receiving mail. With the steady growth of electronic communication and commerce, consumers and businesses need a secure way to communicate and conduct business electronically. Without trustworthy channels of communication, many potential participants in electronic commerce are unwilling to send sensitive information,

e.g., credit card numbers, electronically, thus limiting the utility of electronic commerce to all individuals.

Electronic mail, or e-mail, is a well-known means of communication for individuals and businesses with access to computers and Internet connections.

5 When a user establishes an account with an e-mail service provider, e.g., America Online™ or Hotmail™, the user is assigned a unique e-mail address, e.g. joesmith@aol.com. Another individual can send a message to the user by entering the user's e-mail address along with the message and sending it via the Internet. E-mail can provide almost instant message delivery among individuals and businesses over vast distances for very little or no cost. E-mail also presents an opportunity for businesses to advertise to potential customers in a new way, e.g., by sending bulk advertisements via e-mail.

10
15 Despite the advantages of e-mail, there are several drawbacks. Because e-mail is received and viewed electronically, e-mail does not reach those who are not "online." In this way, e-mail contributes to the so-called "technology gap" between individuals with access to computers and computer technology and individuals who cannot afford or who do not understand computers and computer technology.

20 Additionally, the simplicity and low cost of e-mail make it an easy vehicle for unwanted messages, e.g, unsolicited advertisements or "spam." Both individuals and businesses demand the capability to inhibit the receipt of unwanted e-mail.

Furthermore, e-mail messages are also insecure, and can be intercepted en route by unknown third parties. Businesses and consumers who communicate electronically need to know that their messages are private, and that they can rely on the address to correctly identify the sender and/or recipient.

Therefore, it is desirable to provide a system for communicating electronically that is available to everyone, that gives consumers control over the content of communications received, and that provides a secure and reliable way to conduct transactions electronically.

III. SUMMARY OF THE INVENTION

Systems and methods consistent with the present invention overcome the shortcomings of conventional systems by establishing an electronic account for a customer on a network, where the customer's electronic address is linked to the customer's physical address. As with a conventional electronic account, a customer is able to send and receive e-mail, as well as conduct electronic transactions. However, the electronic account ensures flexible and secure communications by linking a customer's electronic address to the customer's physical address. Systems and methods consistent with the present invention may be implemented by the USPS. Moreover, such a USPS electronic account may provide electronic access to all persons, i.e., a person with a USPS physical address may also have a USPS electronic account.

5 A method consistent with the present invention issues a digital certificate for a user on a network in response to receiving a request for a digital certificate for the user having an electronic account, wherein the electronic account is linked to a physical address of the user. A certificate authority generates the digital certificate for the user, wherein the digital certificate includes information enabling authentication of a transaction on the network, and the digital certificate is linked to the electronic account of the user.

10 Another method consistent with the present invention processes a request for a digital certificate from a user. A proofing workstation receives user information for a user with an electronic account, wherein the electronic account is linked to a physical address of the user. The proofing workstation also receives identification information from the user. The user information is matched to the identification information by the proofing workstation, and an identification verification is sent from the proofing workstation to a proofing server, when the user information has been matched to the identification information.

15 It is to be understood that both the foregoing general description and the following detailed description are exemplary and explanatory only and are not restrictive of the invention, as claimed.

20
IV. BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate several embodiments of the invention and, together with the description, serve to explain the principles of the invention.

In the drawings:

Figure 1 is a high level block diagram of a system for providing an electronic account to a customer;

Figure 2 is a high level block diagram of a system for linking an electronic address to a physical address of a customer;

Figure 3 depicts one embodiment of a link between an electronic address and a physical address of a customer;

Figure 4 is a high level block diagram of a system for providing services to a customer using an electronic account consistent with the present invention;

Figure 5A is a high level block diagram of a system for establishing an electronic account for a customer;

Figure 5B illustrates an embodiment of an identity validation (IDV) form consistent with the present invention;

Figure 6 is a more detailed diagram of a system for establishing an electronic account for a customer;

Figure 7 is a block diagram of an application server consistent with the present invention;

Figure 8 depicts an embodiment of an electronic account number consistent with the present invention;

5

10

15

20

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

Figure 9 is a flowchart of an address matching process performed by a registration system consistent with the present invention;

Figure 10 is a block diagram of standardized address information processed by an address matching engine consistent with the present invention;

Figure 11A depicts an embodiment of the relationship between an ICRS database and a master address database;

Figure 11B depicts an alternative embodiment of the relationship between an ICRS database and a master address database;

Figure 11C depicts another alternative embodiment of the relationship between an ICRS database and a master address database;

Figure 12 is a block diagram of a bulk mailing service using an Internet customer registration system consistent with the present invention;

Figure 13 is a block diagram of services using a customer registration system consistent with the present invention;

Figure 14 is a block diagram of services that can be provided as part of an electronic mailbox consistent with the present invention;

Figure 15 is a block diagram of an advertisement filtering service that can be provided as part of an electronic mailbox consistent with the present invention;

Figure 16 is a block diagram of an e-mail service that can be provided as part of an electronic mailbox consistent with the present invention;

5

10

15

20

Figure 27 is a flowchart of bill delivery notification consistent with the present invention;

Figure 28 is a flowchart of an embodiment in which the EBPP system stores bill summaries and bill details;

Figure 29 is a flowchart of an embodiment in which the biller stores bill details;

Figure 30 is a flowchart of an embodiment in which an EBPP system is provided by a third party and offered to the payer via the electronic account system;

Figure 31 is a flowchart for processing an electronic payment consistent with conventional systems;

Figure 32 is a flowchart of one embodiment of a method for processing an electronic bill payment method using the present invention;

Figure 33 is a flowchart of another embodiment of an electronic bill payment method consistent with the present invention;

Figure 34 illustrates additional services that can be provided through an electronic account consistent with the present invention;

Figure 35 is a block diagram of a system for providing a certificate authority for proofing identities consistent with the present invention;

Figure 36 is a block diagram of a digital certificate consistent with the present invention;

5

10

15

20

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

5

10

15

20

LAW OFFICES
GAGAN, HENDERSON,
ABOW, GARRETT,
DUNNER, L.L.P.
101 STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

Embodiments described herein include systems and methods for providing an electronic account to a customer, linking a customer's electronic address to a physical address of the customer, establishing an electronic account using an Internet Customer Registration System, providing a secure electronic mailbox, and providing a certificate authority for proofing identities.

- 10 -

5 Figure 1 is a high level block diagram of a system for providing an electronic account to a customer. A customer 100 can use a computer, e.g., a personal computer, to log onto a network 102, such as the Internet, to establish an electronic account 104. Electronic account 104 enables customer 100 to access a wealth of electronic services, including e-mail and electronic transactions. These services can be both secure and non-secure and can be provided by any service provider, such as an online merchant, a government agency, or a bank.

10 When electronic account 104 is established, it is linked to a physical address of customer 100. Typically, the physical address corresponds to a location where the user receives physical mail, such as via the USPS or other entity. In this way, anyone who receives mail at a physical address can establish an electronic account consistent with the present invention. The physical address can be a home address, Post Office box, business address, etc.

15 Electronic account 104 can also include an electronic address, such as an e-mail address, for customer 100.

20 To provide electronic services to customer 100, a service provider can communicate with customer 100 via electronic account 104. If electronic account 104 is linked to customer 100's physical address and e-mail address, the service provider can send a communication to electronic account 104 and request delivery to either the physical address or the e-mail address, or both. If such a communication directed to customer 100 contains an incomplete

5

10

15

20

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
2	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56	58	60	62	64	66	68	70	72	74	76	78	80	82	84	86	88	90	92	94	96	98	100	102	104	106	108	110	112	114	116	118	120	122	124	126	128	130	132	134	136	138	140	142	144	146	148	150	152	154	156	158	160	162	164	166	168	170	172	174	176	178	180	182	184	186	188	190	192	194	196	198	200
3	3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	99	102	105	108	111	114	117	120	123	126	129	132	135	138	141	144	147	150	153	156	159	162	165	168	171	174	177	180	183	186	189	192	195	198	201	204	207	210	213	216	219	222	225	228	231	234	237	240	243	246	249	252	255	258	261	264	267	270	273	276	279	282	285	288	291	294	297	300
4	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124	128	132	136	140	144	148	152	156	160	164	168	172	176	180	184	188	192	196	200	204	208	212	216	220	224	228	232	236	240	244	248	252	256	260	264	268	272	276	280	284	288	292	296	300																									
5	5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100	105	110	115	120	125	130	135	140	145	150	155	160	165	170	175	180	185	190	195	200	205	210	215	220	225	230	235	240	245	250	255	260	265	270	275	280	285	290	295	300																																								
6	6	12	18	24	30	36	42	48	54	60	6																																																																																									

20

LAW OFFICES
EGAN, HENDERSON,
RABOW, GARRETT,
DUNNER, L.L.P.
100 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

5

15

20

5

10

15

20

LAW OFFICES
GAN, HENDERSON,
ABOW, GARRETT,
DUNNER, L. L. P.
O I STREET, N. W.
INGTON, DC 20005
02-408-4000

user at a physical address. The physical address can be one provided by the customer with the registration information. Mailpiece 508 contains an identity validation (IDV) form 510, described with regard to Figure 5B below. To complete the registration process, customer 502 takes IDV form 510 to a registration office, such as a local Post Office. There, a clerk verifies the customer's identity and uses IDV form 510 to send identification verification information to registration system 506.

Figure 5B illustrates an embodiment of an identity validation (IDV) form consistent with the present invention. As described above, mailpiece 508 containing IDV form 510 is sent to the customer by registration system 506. When the customer takes IDV form 510 to an identity proofing location, e.g., a local Post Office, a clerk validates the customer's identity and transmits a confirmation to registration system 506.

As shown in Figure 5B, IDV form 510 can include the customer's physical address, the customer's e-mail address, the location of the nearest registration office, and a date by which the customer must go to the registration office. IDV form 510 can also include a list of identity validation documents that the customer must present at the registration office, such as a driver's license, birth certificate, or utility bill. In one embodiment, the customer can select the identity validation documents when submitting registration information to registration system 506.

5

10

15

20

5 IDV form 510 can include a confirmation bar code. The confirmation bar code can be created by the registration system 506 and linked to the electronic account when IDV form 510 is created. Once a clerk validates the customer's identity, for example, by examining the identity validation documents, the clerk can scan the confirmation bar code and send it electronically to registration system 506. When registration system 506 receives the scanned confirmation bar code, the customer's electronic account can be activated. Activation can occur, for example, by sending a digital certificate, password, or other notification to the customer.

10 In one embodiment of the present invention, two copies of IDV form 510 are sent to the customer: one copy for the customer to take to the registration office and another copy for the customer to retain for his records. IDV form 510 can include a set of instructions and a customer care telephone number that the customer can call if he has any problems. IDV form 510 can also include a signature and date block for the customer to execute as part of the identification validation process at the registration office.

15 Figure 6 is a more detailed diagram of a system for establishing an electronic account for a customer. As described above, customer 502 provides registration information to registration system 506 via network 504. Registration system 506 includes an application server 602, a web server 604, and a database server 606. Application server 602 includes software tools to generate dynamic content and execute applications for registration system 506.

20

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

Application server 602 is described in more detail below with reference to Figure 7. Web server 604 processes HTML requests to enable communications with customer 502 and to provide data to application server 602 and database server 606.

Database server 606 processes all communications with an Internet Customer Registration System (ICRS) database 608. In one embodiment, ICRS database 608 consists of two logical components: a customer name database 610 and a customer address database 612. Customer name database 610 stores the registration information provided by a customer along with an electronic account number assigned to the customer. Customer address database 612 stores the customer's physical address. In this embodiment, the physical address is stored separately from the customer's name and other information to protect the security of the customer. To create a high level of security, packet filter access can be installed between customer name database 610 and customer address database 612. Consistent with the present invention, the ICRS database could be maintained as a single database.

When registration system 506 receives registration information from customer 502, it stores the registration information in ICRS database 608 as described above. An identification verification (IDV) form generator 614 then extracts data from ICRS database 608 and passes the data to a print and insertion function 616 that generates mailpiece 508 containing IDV form 510. Alternatively, IDV form generator 614 and print and insertion function 616 can be

5

10

15

20

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

5

10

20

example, a public key and information provided by customer 502 during the registration process.

A digital certificate is a well-known tool for sending secure messages. A CA issues an encrypted digital certificate containing a customer's public key and a variety of other identification information. The Certificate Authority makes its own public key available through print or perhaps on the Internet. The recipient of an encrypted message uses the CA's public key to decode the digital certificate attached to the message, verifies the digital certificate as issued by the CA, and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

Figure 7 is a block diagram of an application server consistent with the present invention. Application server 602 includes application server software 702, certificate software 704, and address matching engine delivery point/plus 4 (AME DP/+4) system software 706. Application server software 602 processes logic and instructions to support registration system 506. Application server software 702 also includes account number generator software 708 that generates an electronic account number for a customer. In one embodiment, account number generator software 708 is embedded into application server software 702 in the form of a dynamically loadable library so that it becomes part of application server software 702 at run time. In another embodiment, account number generator software 708, can be stand-alone software for generating

5
10
15

20

20

LAW OFFICES
 GAN, HENDERSON,
 ABOW, GARRETT,
 DUNNER, L.L.P.
 101 STREET, N. W.
 NGTON, DC 20005
 202-408-4000

Figure 8 depicts an embodiment of an electronic account number consistent with the present invention. In one embodiment, account number

delivery point identification (DPID) key that points to the location in AMD database 908 where the standardized address can be found. Standardized address information 910 is passed back to address matching engine 904, where it can be sent to ICRS database 608. If a DPID key cannot be determined via the address matching engine process, a flag can be set to send feedback to an address management office or other service personnel.

Figure 10 is a block diagram of standardized address information processed by an address matching engine consistent with the present invention. Standardized address information 910 can include a standardized address and related information, including a DPID key. The DPID key can be used to access a storage location in a master address database as described below. The DPID key can be stored with the electronic account information in ICRS database 608.

Figure 11A depicts an embodiment of the relationship between an ICRS database and a master address database. ICRS database 608 can store a DPID key with a customer's electronic account information. To obtain updated address information, ICRS database 608 can use DPID key 1102 to access master address database 1104 and obtain the address 1106 corresponding to DPID key 1102. In this way, an electronic account system consistent with the present invention can perform periodic address updates and quality control processes on ICRS database 608. Using the DPID key in this embodiment keeps ICRS database 608 up-do-date with having to perform multiple address matching engine processes (as described in Figure 9).

5

10

15

20

Figure 11B depicts an alternative embodiment of the relationship between an ICRS database and a master address database. If ICRS database 608 does not store a DPID key with a customer's electronic account information, it can obtain one by submitting a physical address 1108 to a static monolithic address database 1110. Static monolithic address database 1110 can then use an address matching engine (as described in Figure 9) to obtain a DPID key 1112 from master address database 1104. DPID key 1112 is then returned to ICRS database 608.

Figure 11C depicts another alternative embodiment of the relationship between an ICRS database and a master address database. If ICRS database 608 does not store a DPID key with a customer's electronic account information, it can send a physical address 1114 directly to master address database 1104. DPID key 1116 is then returned to ICRS database 608.

3. Services Based on Internet Customer Registration System

Figure 12 is a block diagram of a bulk mailing service using an Internet customer registration system consistent with the present invention. As described above, customer 502 uses a computer to access registration system 506 via network 504. Registration system 506 includes ICRS database 608, which can be accessed by an e-mailbox repository 1210 to provide e-mail services to customer 502. A sender wishing to communicate with a plurality of customers having electronic accounts can submit a file 1202 containing a physical address

file and a content file. The physical address file can be, for example, a mailing list, and the content file can be, for example, an advertisement.

The physical address file is processed in an address matching system 1204 as described above to obtain standardized physical addresses for the customers. The standardized physical addresses are processed by a key generator 1206 to obtain keys for accessing ICRS database 608. Using keys created by key generator 1206, ICRS database 608 is queried at 1208 to create an e-mail address mailing list 1210 corresponding to the physical address file. The content file is combined with e-mail address mailing list 1210 to facilitate an electronic mailing 1212. Electronic mailing 1212 is sent to an e-mail routing system 1214 that sends electronic mailing 1212 to e-mailbox repository 1216 for delivery to the plurality of customers. E-mail routing system 1214 may also provide a status report of e-mail delivery to the sender that provided file 1202.

Figure 13 is a block diagram of services using a customer registration system consistent with the present invention. Electronic account 104 and registration system 506 can enable customers to access an electronic mailbox (or e-mailbox) service 1302 and other services 1304 such as mailing online, electronic bill presentment and payment, etc. Electronic mailbox services 1302 can include a secure electronic mailbox, described in more detail below.

Figure 14 is a block diagram of services that can be provided as part of an electronic mailbox consistent with the present invention. E-mailbox service 1302 can receive and store different types of messages, including advertisement

5

10

15

20

09/675,677 entitled Systems and Methods for Authenticating an Electronic Message, filed on September 29, 2000 and incorporated herein by reference.

Figure 18 is a block diagram of a secure electronic mailbox that can be provided as part of an electronic mailbox consistent with the present invention.

The secure electronic mailbox service is described in more detail below with reference to Figure 20.

4. User Interfaces for Internet Customer Registration System

Figures 19A-19W are screen shots of a user interface for a registration system consistent with the present invention. These screen shots can be, for example, HTML documents stored in registration system 506 and presented by web server 604 to customer 502 at a computer running a browser. Although these user interfaces describe the registration and activation processes in terms of a secure electronic mailbox, these processes can also be used to establish an electronic account consistent with the present invention.

Figure 19A includes an overview of a secure electronic mailbox as provided by the USPS consistent with the present invention. Although the figures describe an electronic account system provided by the USPS, the present invention could be practiced by a non-USPS entity without departing from the spirit and scope of the invention. Figures 19B and 19C contain instructions to the customer for establishing an electronic account using registration system 506. Figures 19D-19F contain a sample privacy and certification policy for use with an electronic account system.

5 Figure 19G is a user interface for collecting registration information from a customer consistent with the present invention. The user interface shown has two sections: individual information and e-mail address selection. The individual information section provides text boxes and/or drop-down lists for the customer to enter: full name, including first name, middle initial, and last name; title, such as Mr. or Miss; suffix title, such as Jr., Sr., II or III; date of birth, including month, day, and year; home phone; and work phone. The e-mail address selection section includes text boxes and/or drop-down lists for the customer to enter a first, second, and third choice of a vanity e-mail address along with a password for the e-mailbox. The user interface asks the customer to reenter the password to ensure that it is accurately captured. This section also enables the customer to choose a shared secret, which can consist of an adjective, a noun, and a verb. The shared secret can serve as a master password for the registration system and helps to identify the customer in the future. For example, the shared secret can be used by the customer to gain access to the customer's digital certificate later in the registration process.

10
15
20 Figure 19H is a user interface that is displayed to the customer if the vanity e-mail address selected is unavailable. The user interface can offer suggestions of available e-mail addresses and a text box to receive the customer's alternate selection.

Figure 19I is a user interface for obtaining physical address information from the customer. The user interface provides text boxes and/or drop-down

5

10

20

embodiment, if the address matching system could not resolve the physical address to a delivery point or plus 4 level, asterisks and a message can be displayed to inform the customer that the physical address is not fully resolved.

Figure 19L is a user interface for explaining a private key system to the customer. The private key is to be generated by browser software running on the customer's computer at the direction of the registration system. The private key will be used by the customer to access the digital certificate to activate the customer's electronic account. The user interface presents a drop-down list for the customer to select an encryption strength, if the customer's browser supports different levels of encryption.

Figure 19M is a user interface for generating a private key for the customer. This user interface enables the customer to click 'okay' to continue with the private key process or to click 'cancel' to stop.

Figure 19N is a user interface for establishing a password for the customer's private key. Because the private key will enable access to the customer's digital certificate, and therefore the electronic account, the customer is encouraged to establish a password to protect the private key. This user interface enables the customer to select a password and enter a confirmation copy of the password before continuing.

Figure 19O is a user interface presented to a customer declining to establish a password for the private key. This user interface informs the customer that a password can be established at a later time and enables the

customer to continue the registration process without establishing a password for the private key.

Figure 19P is a user interface for instructing the customer about the in-person identity validation process. Once the online application process, or registration process, is complete, a temporary or inactive status is assigned to the customer's electronic account. This user interface displays a date on which an identity validation form will be mailed to the customer and explains that the customer will need to take the identity validation form and the chosen identification documents to a registration office to complete the in-person identity validation process.

Figure 19Q is a user interface for beginning the activation process for the customer's electronic account. Once the customer completes the in-person identity validation process, the customer can activate the electronic account. To begin the activation phase, the customer can use this user interface to enter the vanity e-mail address.

Figure 19R is a user interface for capturing the customer's shared secret to activate the customer's electronic account. The customer is prompted to enter the shared secret selected during the online registration process.

Figure 19S is a user interface for accepting a certification practice statement. A certification practice statement is a statement of rules and regulations governing the use of a digital certificate. Once the customer has

read the statement, he can click the 'accept' button to continue or the 'quit' button to stop.

Figure 19T is a user interface for presenting a digital certificate to the customer. This user interface displays a name for the digital certificate and enables the customer to provide a different name, if desired.

Figure 19U is a user interface for saving the digital certificate. The user interface explains the importance of saving a copy of the digital certificate and enables the customer to save it in a safe location or on a floppy disk, for example. The digital certificate can be downloaded into the customer's browser, onto a Smart Card, or onto a digital certificate holding device.

Figure 19V is a user interface for activating the electronic account. Once the customer has received the digital certificate, this user interface enables the customer to confirm that the digital certificate has been installed properly on his computer. A customer care phone number is displayed in case the customer has any problems.

Figure 19W is a user interface for completing the electronic account registration process. This user interface displays a message informing the customer that the electronic account has been activated.

E. Providing a Secure Electronic Mailbox

1. Overview of Secure Electronic Mailbox

One of the services available through an electronic account consistent with the present invention is a secure electronic mailbox (SEM). The SEM can

5 be provided as part of an e-mailbox linked to the electronic account as described
above. Electronic messages can be sent to a customer using the SEM. Unlike a
conventional electronic mailbox, the SEM can provide a number of services in
addition to receiving and displaying electronic messages. For example, the SEM
can enable filtering of messages, notification when a message is received and/or
viewed, and electronic bill presentment and payment. The SEM can offer
various levels of security using, for example, message authentication, time and
date seals, and digital certificates.

10 Figure 20 depicts some classes of messages that can be processed by a
secure electronic mailbox (SEM). SEM 2002 can process a bill, such as a
mortgage bill, utility bill, etc. from a biller 2004, i.e., a biller, a biller's
representative, or a biller service provider. SEM 2002 can process bills from a
plurality of bill consolidators 2006 and 2008. SEM 2002 can also process legal
communications and legal documents 2008, such as patent applications, wills,
etc. Other documents 2010 can also be processed by SEM 2002. In one
embodiment of the present invention, all of a customer's bills (regardless of their
source) are consolidated and presented to the user with a single user interface,
or bill manager. Similarly, payment options can be consolidated and presented
to the user with a single user interface, or payment manager. In this
20 embodiment, a customer can manage all of his bills in one, seamless interface,
without having to know the source of the bills.

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-406-4000

5

10

15

20

5

10

15

LAW OFFICES

- 36 -

the message. The sender can use the secure electronic mailbox to send a message to a recipient at a physical and/or electronic address. Once the message is addressed (i.e., to either a physical or an electronic address), the user can send the message (step 2244).

To send the message, the customer can select delivery options (step 2246), including options such as "delivery notification" or "electronic delivery." If the addressee of the message has an electronic account, the customer can choose "physical delivery" and the message will be printed and delivered in physical form to the addressee's physical address. In addition to delivery options, the customer can select a priority (step 2248) such as "high priority" or "urgent." The customer can choose to postmark the message with an EPM. The customer can also choose to encrypt the message (step 2250) before it is sent. This allows the customer to encrypt a message for privacy and to prevent a third party intercepting the message from reading it. The user can choose to sign the message (step 2252), for example, by attaching a digital signature to the message. Then, the message is sent (step 2253).

If the customer chooses to view a message (step 2240), the customer can select a service to detect tampering (step 2254). This allows the customer to verify whether a message has been tampered with since it was signed by the sender. The tampering detection process can access a secure time and date seal function (step 2256) such as an electronic postmark (EPM) system as described in U.S. Patent Application No. 09/675,677, entitled Systems and

5

10

15

20

electronic address books, which can be stored in an Address Database 2270.

An electronic postmark (EPM) system 2256 can be used to enable the customer to attach a time and date seal (e.g., an EPM) to a message and to detect when a message with a time and date seal (e.g., an EPM) has been tampered with. A

5 Sign and Encrypt component 2272 can be used to enable a customer to digitally sign messages.

3. Electronic Bill Presentment and Payment

A secure electronic mailbox consistent with the present invention supports many services in addition to electronic message handling. A customer with an electronic account can use an electronic bill presentment and payment (EBPP) service to receive and pay bills electronically. Billers, such as utility companies or credit card companies, can join the EBPP system and submit bills, bill summaries, bill histories, etc. to the customer (i.e., the payer) using the electronic account and SEM systems. An EBPP system consistent with the present invention improves upon conventional electronic bill payment systems in several ways. First, the present invention uses an EBPP system to improve communication and feedback between a biller and a payer. Second, an EBPP system consistent with the present invention is linked to a physical address of the payer enabling flexible communications including physical and electronic mail. Third, because an EBPP system consistent with the present invention is linked to a payer's electronic account, the biller knows that the identity of the

10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100

payer was verified in person and therefore can be more confident in sending bills and receiving payment via the EBPP system. Fourth, bills from several sources can be consolidated for viewing seamlessly, i.e., without indicating the source of the bill. Payment can be provided to the appropriate biller seamlessly, i.e., without indicating the payment destination to the customer.

Figure 23 is a flowchart of a process for a customer to enroll in an electronic bill presentment and payment system consistent with the present invention. A payer having an electronic account can send a message requesting enrollment in an electronic bill presentment and payment (EBPP) system (step 2302). The enrollment request can be sent to a secure electronic mailbox (SEM) system consistent with the present invention. If the enrollment request includes a reference to a bank account of the customer, then the EPBB system can access that bank account to automatically pay bills for the payer. The SEM system authenticates the payer using, for example, the digital certificate from the payer's electronic account (step 2304). The authentication process is described in more detail below. When the payer is authenticated, the SEM system retrieves information about the payer, for example, from the payer's electronic account, and sends the enrollment request and payer information to an EBPP system (step 2306). In one embodiment, the EBPP system can send the enrollment request and payer information to a biller and receive an enrollment status from the biller. Once the EBPP system establishes and activates an

5

10

15

20

EBPP account for the payer, the enrollment status is sent from the EBPP system to the SEM system (step 2308) and then to the payer (step 2310).

In an alternative embodiment, the enrollment request can also be initiated by a biller. For example, a payer could sign up for the EBPP system at a biller's web site. The biller-initiated enrollment request would then be sent from the biller to the EBPP system (step 2312) and the biller-initiated enrollment status can be returned to the biller (step 2314).

Figure 24 is a flowchart of a process for a customer to activate an electronic bill presentment and payment account consistent with the present invention. After the enrollment process, the payer can request activation of the EBPP account by sending an account activation request to the SEM system (step 2402). Before processing the request, the SEM system can authenticate the user with a certificate authority as described below (step 2404). Once the payer is authenticated, the account activation request is sent from the SEM system to the EBPP system along with information from the payer's electronic account (step 2406). The account activation request is then sent to a biller (step 2408). When the biller activates the payer's account, a response is sent from the biller to the EBPP system (step 2410). The EBPP system sends the account activation status to the SEM system (step 2412) and the SEM system sends it to the payer (step 2414). The biller could also send out a physical notification of the account activation status directly to the payer (step 2416). In an

10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
160
170
180
190
200
210
220
230
240
250
260
270
280
290
300
310
320
330
340
350
360
370
380
390
400
410
420
430
440
450
460
470
480
490
500
510
520
530
540
550
560
570
580
590
600
610
620
630
640
650
660
670
680
690
700
710
720
730
740
750
760
770
780
790
800
810
820
830
840
850
860
870
880
890
900
910
920
930
940
950
960
970
980
990
1000

alternative embodiment, account activation could be initiated by the biller and the biller can be notified of the account activation (step 2418).

Figure 25 is a flowchart of a process for a biller to register for an electronic bill presentment and payment system consistent with the present invention. To register, a biller sends biller registration information to the electronic bill presentment and payment (EBPP) system (step 2502). The EBPP system processes the biller registration information and sends it through general administrative and marketing processing (step 2504). This step may include, for example, verifying the biller's taxpayer ID number or other identifier or evaluating the biller's accounting software. Once the biller is registered, the EBPP system sends a registration completion notification to the biller (step 2506). Marketing or advertisements can also be sent from the EBPP system to the biller.

Figure 26 is a flowchart of a process for presenting bills to a customer using the electronic account system. In one embodiment, a biller can submit bill summaries for multiple customers to the electronic account system (step 2602) via a network such as the Internet. Each bill summary may be marked with an EPM and can be stored in a SEM corresponding to a specific customer. When a customer logs into his SEM (step 2604), the customer can view the bill summary (step 2606). The bill summary may be marked with an EPM. The customer can then request, via the SEM system, to view bill details (step 2608). The bill details may be marked with an EPM. The customer can also link directly with the biller

5

10

15

20

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N.W.
WASHINGTON, DC 20005
202-408-4000

5

15

There are many alternative embodiments for storing and presenting bill information to the payer. The electronic account system can store all bill information in the EBPP system (e.g., to bill for SEM services). Alternatively, the EBPP system may store only bill summary information and the payer can communicate directly with a biller to obtain bill details. In another embodiment, the EBPP system may be provided by a third party and offered to the payer via the electronic account system.

Figure 28 is a flowchart of an embodiment in which the EBPP system stores bill summaries and bill details. The payer can access his SEM to view bill summaries (step 2802) and to view bill details, historical bills, and/or payment information (step 2804). When the payer accesses the SEM, the payer will be authenticated using, for example, a certificate authority (step 2806). In this embodiment, the SEM obtains bill detail (i.e., line by line bill details) and bill summary information (e.g., overall balance due, biller identifier, etc.) from the EBPP system, stored within the electronic account system (steps 2808, 2810). The payer can also obtain historical information such as payment history and past bills.

Figure 29 is a flowchart of an embodiment in which the biller stores bill details. The payer can access his SEM to view bill summaries (step 2902), bill detail, historical bills and/or payment information (step 2904). When the payer accesses the SEM, the customer will be authenticated using, for example, a

certificate authority (CA/PKI) (step 2906). In this embodiment, the SEM obtains bill detail (i.e., line by line bill details) and bill summary information (e.g., overall balance due, biller identifier, etc.) from the EBPP system (step 2908), which in turn obtains bill details from a remote biller, e.g., via a network. (step 2910). The payer can also obtain historical information such as payment history and past bills.

Figure 30 is a flowchart of an embodiment in which an EBPP system is provided by a third party 3001 and offered to the payer via the electronic account system. The payer can access his SEM to view bill summaries and bill detail (step 3002) and to view historical bills and/or payment information (step 3004). The bills may be issued by a plurality of billers, but the bills can be consolidated and presented to the payer using a single, seamless user interface. When the payer accesses the SEM, the customer will be authenticated using, for example, a certificate authority (step 3006). In this embodiment, the SEM obtains bill detail (i.e., line by line bill details) and bill summary information (e.g., overall balance due, biller identifier, etc.) from a third-party EBPP system (step 3008), which in turn obtains bill details from a remote biller, e.g., via a network. (step 3010). The payer also can also obtain historical information such as payment history and past bills.

Figure 31 is a flowchart for processing an electronic payment consistent with conventional systems. To pay a bill electronically, a payer sends payment

5 authorization to a financial processor such as, for example, Checkfree (step 3102). The financial processor sends the payment authorization to the payer's bank (step 3104). The payment authorization can include a payer's bank account designation and a biller's bank account number. The payer's bank can send payment to the biller's bank (step 3106), e.g., by electronically transferring money to the biller's bank account. The payer's bank can then send a transaction confirmation to the financial processor (step 3108). Alternatively, the financial processor can send payment directly to the biller's bank (step 3110). The financial processor can send the transaction confirmation to the payer (step 3112). Once payment is received, the biller's bank can send payment notification to the payer (step 3114).

10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995

Figure 32 is a flowchart of one embodiment of a method for processing an electronic bill payment method using the present invention. A payer sends payment authorization to his SEM (step 3202). The SEM can apply an electronic postmark (EPM) to the payment authorization for added security (step 3204). The SEM sends the payment authorization to the EBPP system (step 3206), which is part of the electronic account system in this embodiment. The EBPP system in turn sends the payment authorization to a financial institution (step 3208). This method is an improvement over conventional systems in many ways. The inclusion of an EPM on the payment authorization enhances security for both payer and biller. Because the identity of the payer is validated before

the SEM is activated, the biller has increased confidence when sending bills and receiving payment.

Figure 33 is a flowchart of another embodiment of an electronic bill payment method consistent with the present invention. A payer sends payment authorization to his SEM (step 3302). The SEM can apply an electronic postmark (EPM) to the payment authorization for added security (step 3304). The SEM sends the payment authorization to the EBPP system (step 3306), which is not part of the electronic account system in this embodiment. The EBPP system in this embodiment could be offered by a third party to the payer via the electronic account system. The EBPP system sends the payment authorization to a financial institution (step 3308).

Figure 34 illustrates additional services that can be provided through an electronic account consistent with the present invention. Other services 3402 that can be provided via an electronic account include mailing online 3404, NetPost.Certified 3405, shipping online 3406, stamps online 3408, PC Postage 3409, and other services 3410. Mailing online 3404 is a service that receives a content file and an address list from a customer and produces a mailing to each address on the address list. Mailing online can include a Card Store product. NetPost.Certified 3405 enables a customer to download a digital certificate onto a Smart Card for use in authenticating electronic transactions. Shipping online 3406 is a service that enables a customer to ship packages automatically and

privately. Stamps online 3408 enables a customer to purchase stamps. PC Postage 3408 enables a customer to purchase and print postage using a computer.

F. Certificate Authority for Proofing Identities

Systems consistent with the present invention provide a certificate authority for proofing the identity of an electronic customer. Using digital certificate software, the electronic account system provides a digital certificate, described in detail below, to a customer after the customer has been verified in-person as part of the electronic account registration process. In this way, a digital certificate consistent with the present invention authenticates the customer's identity in a way that is not available in conventional systems.

Figure 35 is a block diagram of a system for providing a certificate authority for proofing identities consistent with the present invention. A digital certificate requestor 3502 sends a request for digital certificate 3504 to a digital certificate authority 3506. Digital certificate requestor 3502 can be, for example, certificate software or a proofing workstation. In response to request for digital certificate 3504, digital certificate authority 3506 sends a digital certificate 3508 to digital certificate requestor 3502.

Figure 36 is a block diagram of a digital certificate consistent with the present invention. Digital certificate 3508 includes an identifier of the customer 3602, a certificate serial number 3604, a certificate validity period 3606, a

5

10

15

20

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

proofing workstation validation 3608, a public key 3610, a certificate issuer identifier 3612, and a certificate status 3614. Certificate status 3614 can be, for instance, active, on hold, or revoked. The digital certificate can be, for example, a well-known CCITT X.500 Section 509 Version 3 certificate.

5

Figure 37 is a block diagram of a certificate authority consistent with the present invention. Certificate authority 3506 contains known software to generate digital certificates as described above. In addition, certificate authority 3506 includes at least one proofing server 3702 and at least one proofing workstation 3704. As described above, a customer having an electronic account can conduct electronic transactions and provide a digital certificate to third parties to verify the customer's identity. A third party can request verification of the digital certificate via proofing workstation 3704, such as a kiosk available in a Post Office. Proofing workstation 3704 communicates with proofing server 3702 to verify the digital certificate and returns the verification to the third party via proofing workstation 3704. Thus, certificate authority 3506 enables third parties to proof the customer's identity using a digital certificate.

10

15

Figure 38 is a block diagram of a proofing server consistent with the present invention. Proofing server 3702 includes a certificate directory 3802, a certificate revocation list 3804, and an interface with proofing workstations 3806. Certificate directory 3802 is a list of digital certificates that have been issued by proofing server 3602, e.g., using known digital certificate software. Certificate

20

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

revocation list 3804 is a list of certificates that have been revoked, e.g., for fraudulent use generated by an electronic account system or a third party. Interface with proofing workstations 3806 includes a private key verifier 3808 that provides security by verifying a private key sent with a verification request from a proofing workstation..

Figure 39 is a block diagram of a proofing workstation consistent with the present invention. Proofing workstation 3704 can be, for example, a computer or kiosk available in a public place, such as a Post Office. A third party wishing to proof a digital certificate can submit a request to proofing workstation 3704, perhaps accompanied by a fee paid by credit card or smart card. Proofing workstation 3704 communicates with proofing server 3702 to proof the digital certificate and return a validation to the third party. Proofing workstation 3704 includes a central processing unit (CPU) 3902, an input device 3904 (e.g., a keyboard), an output device 3906 (e.g., a printer or monitor), an interface with proofing servers 3908, a memory 3910, a credit card reader 3914, and a smart card interface 3916. Memory 3910 includes a private key 3912. Private key 3912 is sent with proofing requests from proofing workstation 3704 to proofing server 3702 to provide security.

While digital certificates consistent with the present invention use in-person identity validation using identification documents, many different types of identity validation may be used consistent with the present invention. For

5

10

15

20

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

5

10